60

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,493	07/06/2001	Michael Freed	NEXSI-01111US0	4137

28863 7590 07/25/2005

SHUMAKER & SIEFFERT, P. A.
8425 SEASONS PARKWAY
SUITE 105
ST. PAUL, MN 55125

EXAMINER	
ALOMARI, FIRAS B	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 07/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/900,493	**Applicant(s)** FREED ET AL.	
	Examiner Firas Alomari	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on *04 April 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-9 and 12-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-9 and 12* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *11/05/2005*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

1. The amendment filed 04-04-2005 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows: Claim 1 recite the limitation "discarding at least a portion of the decrypted unauthenticated packet application data for the security record prior to receiving a final packet of the security record" this limitation is not mentioned in the specification.

Applicant is required to cancel the new matter in the reply to this Office Action.

2. Claims 3, 10 and 11 are cancelled in the Amendment.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 2, 4-9 and 12-20 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 2 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin US (6,681,327) in view of Scholnick US (5,978,918) .

As per claims 1: Jardin disclose

A method for enabling secure communication between a client on an open network and a server apparatus on a secure network (item 100 of FIG. 1), the method performed on a intermediary apparatus coupled to the secure network and the open network (item 120 of FIG. 1), comprising:

- Negotiating a secure communications session with the client apparatus via the open network;(items 210, 220, 230 and 240 of FIG 2; describes the "handshake " between the client and the server which used to start any communication between the server and the client)
- Negotiating an open communications session with the server via the secure network; (Col 6, lines 40-46)
- Receiving encrypted packet application data for a security record spanning multiple data packets, wherein the security record has a length greater than a packet length

associated with the multiple data packet; (Col 6, lines 65-69; The examiner deeming this to be inherent to any TCP/IP system, which split the application data packets to multiple TCP/IP packets to be transmitted over the network.)

- Decrypting the encrypted packet application data in each data packet; (Col 6, line 67)
- Forwarding decrypted, unauthenticated application data to the server via the secure network; (Col 7, line 4)
- Jardin doesn't explicitly teach *discarding at least a portion of the decrypted unauthenticated packet application data for the security record prior to receiving a final packet of the security record and authenticating the data*. However Scholnick discloses a method to secure data transmitted over public networks (Col 1, lines 32-67) where he teaches using of SSL to secure the transmission and he discards a portion of the packet data prior to receiving the final packet segment and authenticating the data (Col 31-39, lines). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Jardin system with the teachings of Scholnick to discard at least a portion of the decrypted packet application data prior to receiving the final data segment because the discarded data is not needed in the authentication process.

As per claim 2: Jardin system discloses

- Forwarding data which spans over multiple TCP segments. (Col 7, lines 44-45)

As per claim 4: Jardin system discloses

- The method of claim *1* wherei*n a remaining portion of the packet application* data for the *security record* is buffered *as a minimal* length sufficient to complete a block cipher used to encrypt the data. (Col 2, lines 65, through Col 3, line 3 / the broker in the second embodiment have dynamically allocated buffer. the broker in the second embodiment have dynamically allocated buffer to. furthermore its well known in the art that in order to perform a block cipher encryption in DES and SSL that the encryption and/or decryption is performed on a block basis and in the last block if the length is insufficient the data is padded to maintain a specific length for the DES to operate on. Therefore for any system performing a SSL and DES have to buffer at least one block of data in order for it to be able to decrypt the data)

As per claims 6:

- *After forwarding the decrypted unauthenticated application data to the server,* notifying the client apparatus if a failure in authenticating *the security record* occurs. The examiner deeming this to be inherent to any SSL based communication systems that utilize an alert protocol that handles all SSL crypto related errors. The "bad_record_mac " error notifies the client if the MAC of the received SSL record is incorrect.

3. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin US (6,681,327) in view of Scholnick US (5,978,918) as applied to claim 1 above, and further in view of Narad et al US (6,157,955).

As per claim 5 :

- The method of claim 1 wherein *authenticating* includes authenticating decrypted data *for the security record upon receiving* a final *TCP* segment of a multi-segment encrypted data stream *and after forwarding the decrypted unauthenticated application data received prior to the final segment.* The combination of Jardin and Scholnick does not explicitly explain a packet authentication. However Narad teach the using and tracking of both a checksum (column 36, lines 40, through column 37, line 20) and a cryptographic key (column 27, lines 4-7) to verify the validity of the data packet. Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Jardin with the teaching of Narad to authenticate received packets after the final packet in the data segment received. One would be motivated to do so in order to identify and discard packets that have been altered or modified.

4. Claims 7-9 and 12-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin US (6,681,327) in view of Narad et al US (6,157,955).

As per claim 7:

A method for processing encrypted data transferred between a first system and a second system, comprising:

- Providing an accelerator device including a decryption engine in communication with the first system via an open network and the second system via a secure network;(item 120 of FIG. 100)
- Receiving encrypted data from the first system via the open network in the form of application data spanning multiple packets, each packet having a packet length and information for authenticating the application data;(Col 6, line 67)
- Decrypting ones of said packets as said packets are received, (Col 7 lines 39-41)
- Forwarding application data as said packets are decrypted to the second device via the secure network; (Col 7, line 4)
- Authenticating the data when said information for authenticating the data is received in a last of said multiple packets. Jardin do not explicitly explain a packet authentication. However Narad teach the using and tracking of both a checksum (column 36, lines 40, through column 37, line 20) and a cryptographic key (column 27, lines 4-7) to verify the validity of the data packet. Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Jardin with the teaching of Narad to authenticate received packets after the final packet in the data segment received. One would be motivated to do so in order to identify and discard packets that have been altered or modified.

As per claim 8: Jardin system teaches

- The method of claim 7 wherein said step of receiving comprises receiving SSL encrypted data. (Col 4, lines 11-12)

As per claims 9,13,17 and 18: Jardin system teaches

- The method of claim 7 wherein said step of decrypting comprises decrypting application data encrypted using SSL, DES and a 3DES algorithm. (Col 5, lines 16-20)

As per claim 12:

- The method of claim 7 wherein buffering comprises buffering the application data for a minimal length sufficient to complete a block cipher used to encrypt the data. (Col 2, lines 65, through Col 3, line 3 / the broker in the second embodiment have dynamically allocated buffer to. furthermore its well known in the art that in order to perform a block cipher encryption in DES and SSL that the encryption and/or decryption is performed on a block basis and in the last block if the length is insufficient the data is padded to maintain a specific length for the DES to operate on. Therefore for any system performing a SSL and DES have to buffer at least one block of data in order for it to be able to decrypt the data)

As per claim 14:

- *Altering the first device if authenticating fails after forwarding the decrypted unauthenticated application data that is received prior to the last one of multiple packets.* The examiner deeming this to be inherent to any SSL based communication systems that utilize an alert protocol that handles all SSL crypto related errors. The "bad_record_mac " error notifies the client if the MAC of the received SSL record is incorrect.

As per claim 15:

- The method of claim 7 wherein authenticating includes generating a reset to the second device if authenticating fails. The examiner is deeming this to be inherent to any SSL communication system, where the authentication failure error message "bad_record_mac " in the SSL protocol is considered fatal and upon receive of the message connection is closed.

As per claim 16: Jardin system teaches

A method of providing secure communications using limited buffer memory in a processing device (Col 6, lines 5-11), comprising:

- Receiving encrypted data having a length greater than a TCP segment carrying said data;(Col 6, line 67)
- Buffering the encrypted data in a memory buffer in the device, the buffer having a length equivalent to the block cipher size necessary to perform the cipher;(Col 6, lines 9-14)

- Decrypting the buffered segment of the received encrypted data to provide decrypted application data;(Col 7 lines 39-41)
- Forwarding the decrypted application data to a destination device. (Col 7, line 4).

As per claim 19 :

- The method of claim 1 wherein *authenticating* includes authenticating decrypted data *for the security record upon receiving* a final *TCP* segment of a multi-segment encrypted data stream *and after forwarding the decrypted unauthenticated application data received prior to the final segment*. Jardin does not explicitly explain a packet authentication. However Narad teach the using and tracking of both a checksum (column 36, lines 40, through column 37, line 20) and a cryptographic key (column 27, lines 4-7) to verify the validity of the data packet. Therefore, it would be obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Jardin with the teaching of Narad to authenticate received packets after the final packet in the data segment received. One would be motivated to do so in order to identify and discard packets that have been altered or modified.

As per claims 20:

- *After forwarding the decrypted unauthenticated application data to the server,* notifying the client apparatus if a failure in authenticating *the security record* occurs.

The examiner deeming this to be inherent to any SSL based communication systems that utilize an alert protocol that handles all SSL crypto related errors. The "bad_record_mac " error notifies the client if the MAC of the received SSL record is incorrect.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached on M-F from 7:30 am - 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari
Examiner
Art Unit 2136

FA

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100